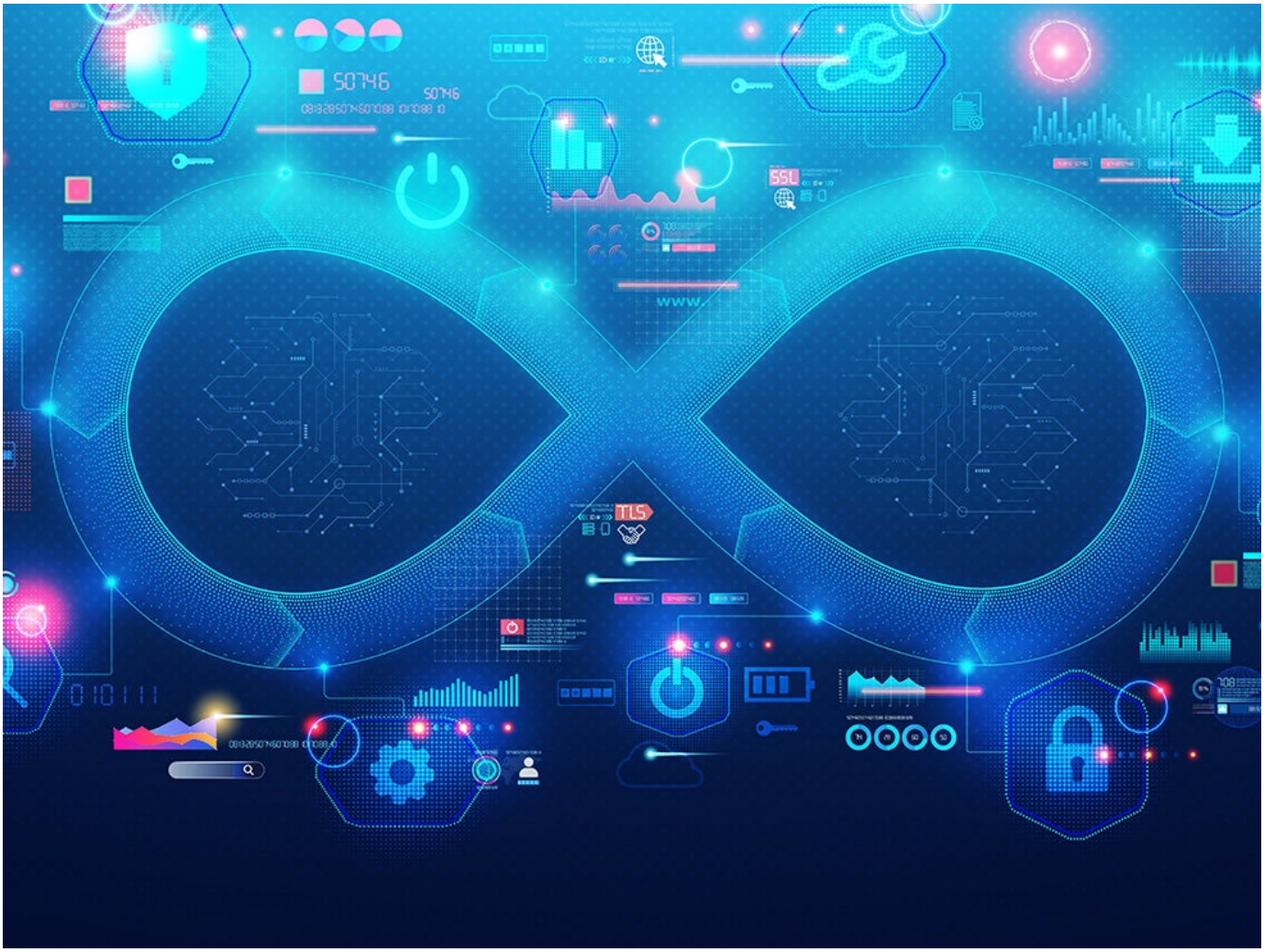
Accelerate Your Secure Toolchain Adoption

June 26, 2023

Cybersecurity Research Analyst

Alex is a cyber security research analyst at Stratascale. His background in both research and practical security gives him a unique perspective on providing security with a risk-based approach. He focuses his expertise on emerging technologies, data-driven IT strategy, and tactical solutions to large security problems.

Submitted by Alex Banghart on 26, Jun 2023
Accelerate Your Secure Toolchain Adoption



Accelerate Your Secure Toolchain Adoption

Executive Summary

Modern enterprises’ digital assets and products have a huge impact on brand, revenue, and reputation. Business and security leaders must ensure the safe and efficient management of these assets in order to maintain a competitive edge in the market.

This requires business and security leaders to prioritize the development of secure applications that not only meet market demands but also safeguard sensitive data and protect against evolving cyber threats. The ability to run fast and safely, with secure applications and speedy feature releases, is paramount to capturing market opportunities and maintaining customer satisfaction.

Leaders must drive secure toolchain adoption

Business and security leaders must spearhead the adoption of secure toolchains within their development organizations. Secure toolchains encompass a set of integrated software development tools and practices that enable teams to build applications with robust security measures ingrained in their DNA. By driving the adoption of secure toolchains, leaders can ensure the consistent implementation of secure coding practices, streamline development processes, and foster a culture of security awareness and accountability throughout their organizations.

To effectively drive secure toolchain adoption, leaders should focus on establishing the necessary skills, automation, and culture within their organizations.

Skills. Leaders must invest in education and training programs to equip their development teams with the necessary knowledge and skills to build secure applications. By promoting a deep understanding of secure coding practices and the potential consequences of security vulnerabilities, leaders can empower their teams to proactively address security concerns during the development process.

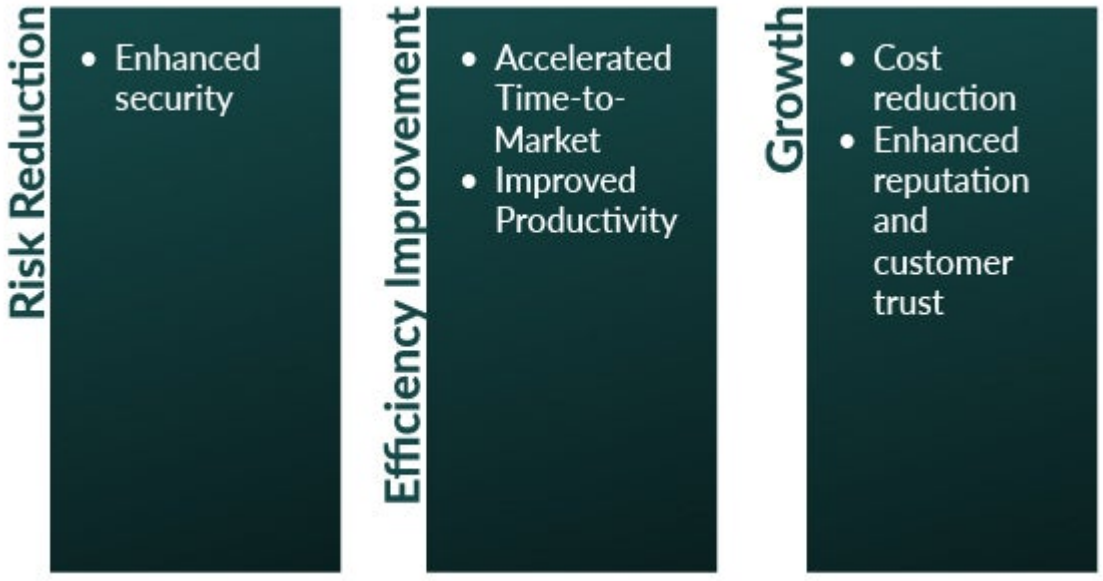
Automation. Integrating security testing and analysis tools into the development pipeline is essential for identifying and mitigating potential vulnerabilities early on. By automating security assessments and code analyses, leaders can enable their teams to detect and remediate security issues in a timely manner, reducing the risk of data breaches and other security incidents.

Culture. Leaders must foster a culture of security awareness and accountability across the organization. This involves promoting open communication channels for reporting and addressing security concerns, establishing security metrics and performance indicators, and rewarding individuals and teams for their commitment to building secure applications. By embedding security as a core value within the organizational culture, leaders can drive long-term adoption and ensure the sustainability of secure toolchain practices.

The benefits of driving secure toolchain adoption are substantial. By implementing secure toolchains, organizations can minimize security risks, reduce the potential for data breaches, and protect their valuable digital assets. Additionally, the streamlined development process enabled by secure toolchains enhances efficiency, reduces time-to-market, and yields cost savings. Furthermore, the establishment of a strong security posture builds customer trust, enhances brand reputation, and positions organizations as leaders in data protection and privacy.

Why drive secure toolchain adoption

DevOps has revolutionized software development by emphasizing the rapid delivery of code into production. However, in today's security-conscious landscape, it is imperative to go beyond speed and prioritize the integration of security practices into the development process. DevSecOps extends the concept of DevOps by not only ensuring quick delivery but also incorporating security measures from the outset. Adopting a secure toolchain enables organizations to achieve these objectives, offering several significant business benefits.



Accelerated Time-to-Market: A secure toolchain automates various security testing and analysis processes, eliminating the need for manual reviews that can be time-consuming and error-prone. By integrating automated security controls into the

pipeline, organizations can quickly identify vulnerabilities and weaknesses in the code, enhancing the overall security posture. This automation streamlines the development lifecycle, allowing businesses to release software updates faster, gain a competitive edge, and capitalize on market opportunities.

Enhanced Security: With automated security testing embedded within the toolchain, organizations can identify and address security vulnerabilities earlier in the development process. By continuously scanning for potential threats, organizations can proactively remediate issues, reducing the risk of data breaches and other security incidents. The toolchain enables developers to have real-time visibility into the security of their code and applications across the Software Development Life Cycle (SDLC), empowering them to take ownership of security and produce more secure code.

To fully harness the benefits of a secure toolchain, it is essential to establish an effective pipeline that encompasses automated testing for security controls. Manual security reviews are not scalable and often introduce delays in the development process. By integrating automated security testing into the toolchain's pipeline, organizations can consistently evaluate the security of their code and applications throughout the SDLC.

Improved Productivity and Efficiency: A secure toolchain provides developers with the necessary resources and tools to be productive quickly. By automating security controls and integrating them seamlessly into the development workflow, developers can focus on writing code without interruptions, knowing that security is being addressed throughout the process. The toolchain also enables efficient collaboration and communication among teams, eliminating the need for manual ticketing systems and enabling faster resolution of security-related issues.

Cost Reduction: Investing in a secure toolchain upfront can result in significant cost savings in the long run. By automating security processes and minimizing the occurrence of security vulnerabilities, organizations can avoid the costly repercussions of data breaches, system downtime, and subsequent remediation efforts. Additionally, the streamlined development process enabled by the toolchain reduces wasted time and resources, optimizing resource allocation and maximizing

overall efficiency.

Enhanced Reputation and Customer Trust: A strong security posture, achieved through the adoption of a secure toolchain, builds customer trust and enhances brand reputation. In an era where data privacy and protection are paramount concerns for customers, demonstrating a commitment to secure coding practices and robust security measures fosters confidence in the organization's products and services. This, in turn, strengthens customer loyalty and helps attract new customers.

Blockers to Adopting a Secure Toolchain

While the adoption of a secure toolchain brings numerous benefits, there are several common blockers that organizations may encounter. Understanding these obstacles is crucial for addressing them effectively and ensuring successful adoption across development teams.

Blocker	Way to overcome
Lack of standardization	Get executive buy-in Implement governance Establish, empower, and fund a service-oriented platform team.
Resistance to change	Effectively communicate benefits Apply organizational change management best practices Establish and empower enterprise transformation office

Existing investments	Demonstrate the advantages of new tools Highlight specific cases where the toolchain can help
Focus on features over security	Get executive buy-in Implement governance (e.g. security metrics for performance reviews)
Usability and Tool quality	Establish, empower, and fund a service-oriented platform team. Bake user-experience/user-centered design capabilities into the platform team to ensure the solution(s) meet developer needs

1. **Lack of Standardization:** The distributed nature of many development organizations, with multiple operating companies, lines of business, and application teams, often results in a lack of standardization. This lack of consistency and uniformity hinders the automation of security practices and the achievement of enterprise-wide visibility into the Software Development Life Cycle (SDLC). When different teams use their own tools, it becomes challenging to establish an integrated and secure toolchain that spans the entire organization.

2. **Resistance to Change:** Developers are driven by productivity and the desire to complete their tasks quickly and efficiently. Introducing a new toolchain can disrupt established workflows and require individuals to adapt to new processes and technologies. General resistance to change can arise from concerns about potential disruptions, learning curves, or perceived inefficiencies. Overcoming resistance requires effective communication, clear benefits, and a strong sponsor/champion who evangelizes the secure toolchain.

3. **Existing Investments in Custom Tools**: Some development teams may have invested time and resources in building their own tools to support their specific needs. They may be reluctant to abandon these custom solutions in favor of a standardized secure toolchain. In such cases, it is crucial to demonstrate the advantages and capabilities of the secure toolchain, highlighting how it can enhance productivity, security, and collaboration across teams.

4. **Focus on Features Over Security:** Developers often prioritize delivering new features and functionality to meet business requirements. Security concerns may take a backseat as developers may perceive security as an additional burden or an impediment to their primary goals. It is essential to convey the importance of security as a fundamental aspect of the development process and demonstrate how a secure toolchain can ensure both feature development and robust security.

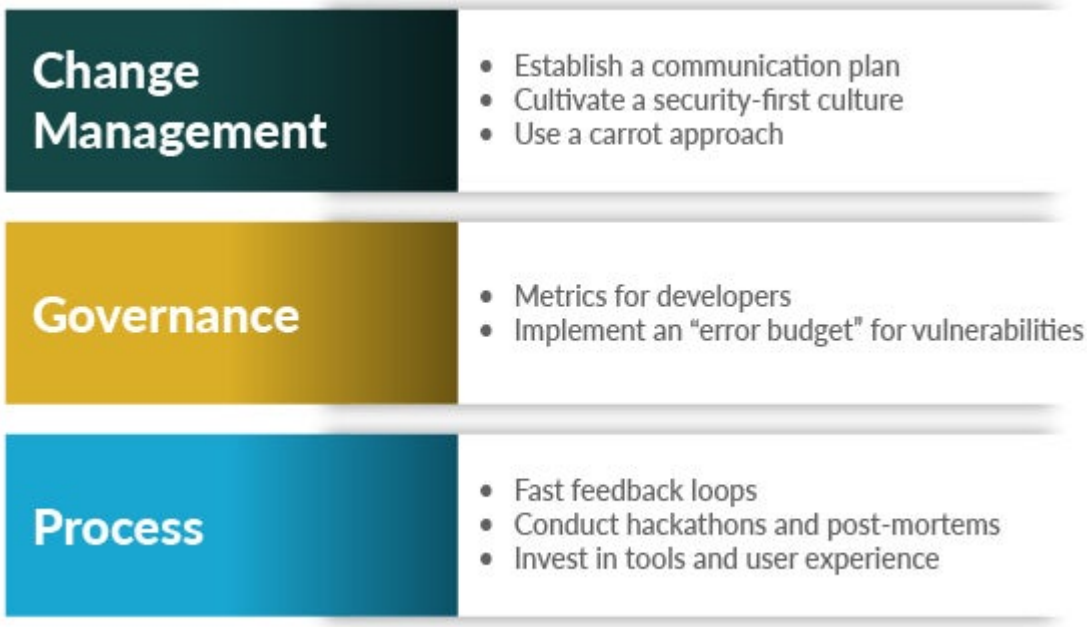
5. **Usability and Tool Quality:** The usability and quality of the tools provided within the secure toolchain can significantly impact adoption. If the tools are difficult to use, lack intuitive interfaces, or do not integrate well with existing workflows, developers may be discouraged from utilizing them.

   It is crucial to ensure that the tools within the toolchain are user-friendly, well-documented, and designed to enhance developer productivity rather than hinder it. Requirements should be built around choosing products and requirements that are baked into tools that are already common in the industry and developers are comfortable using. Mandating requirements that popular tools do not meet can lead to developers being frustrated and unproductive. By developing and reviewing these requirements with your development team they can feel involved in the process, and it fosters cooperation and leaves open room for novelty which is crucial in high-performance organizations.

Addressing these blockers requires a comprehensive approach that addresses the concerns and needs of developers while emphasizing the benefits of adopting a secure toolchain. Providing training and support to help developers understand the value proposition, demonstrating the ease of use and integration capabilities of the tools, and fostering a collaborative environment that encourages feedback and continuous improvement can help overcome these obstacles.

Tips and Tricks to Driving Secure Toolchain Adoption

Driving the adoption of a secure toolchain requires a strategic approach that aligns incentives, fosters a culture of security, and provides the necessary support and resources. Here are several tips and tricks to facilitate the successful adoption of a secure toolchain within development organizations:



Establish a Communication Plan: Develop a comprehensive communication plan that clearly articulates the benefits of adopting a secure toolchain and aligns incentives with the goals of both developers and the organization. Highlight how the toolchain can improve developers' productivity, code quality, and overall security

posture. The graphic below shows how a secure toolchain can help developers improve and meet the four key DevOps Metrics.

Emphasize the alignment of security with quality code and emphasize that secure code is an essential component of delivering high-quality software.

Metrics for Developers: In addition to traditional DevOps metrics, provide developers with specific metrics related to vulnerabilities and vulnerability management.

1. Failed Deployment Rate (FDR): How many releases are blocked from security issues

2. Lead Time for Changes (LTC) How long from initial code commits to running in production

3. Defect Escape Rate: How many security bugs are released into production and how severe are they

4. Defect Volume: How many security bugs are released into the product

5. # of Penetration Test Findings

6. Time To Remediation (TTR) How fast are security issues able to be fixed

By providing metrics that shift security into how developers are measured on their performance you can help drive toolchain adoption by providing the tools to help them meet these goals.

Fast Feedback Loops: Integrate fast feedback loops into the development process by implementing automated security tests that run when code is checked in. When checked-in code fails one or more tests, developers receive immediate feedback on potential security vulnerabilities in their code, enabling them to address issues in a timely manner. Fast feedback loops promote a proactive and iterative approach to security, allowing developers to learn from their mistakes and improve code quality.

Cultivate a Security-First Culture: Instill within the organizational culture the understanding that security is an integral part of producing quality code. Emphasize that while code may function well and deliver intended features, if it lacks security, it becomes a liability. Encourage developers to prioritize security as a core component of their work and provide them with the necessary resources, training, and support to enhance their security knowledge and skills.

Conduct Hackathons and Post-Mortems: Organize hackathons where teams develop applications while other teams attempt to attack those applications (blue teams vs. red teams). This exercise promotes a hands-on understanding of security vulnerabilities and fosters a proactive approach to secure coding. Conduct post-mortems to analyze breaches or security incidents in a blameless manner, focusing on learning and improving security practices rather than assigning blame. Recognize

and reward individuals and teams for their contributions to improving security.

Carrot Approach: To make the organization's toolchain more desirable, specific requirements can be set that align with its capabilities and advantages. These requirements act as a framework that ensures compatibility, integration, and efficient workflows. For example, the requirements may include seamless integration with existing systems, support for collaborative features, and compatibility with key dependencies. Developers who choose their own toolchains must meet these requirements, which may be time-consuming or technically challenging. This approach encourages them to consider adopting the organization's toolchain to enjoy its benefits.

By actively engaging with developers, involving them in the decision-making process, and addressing their concerns, organizations can promote a culture of security and collaboration, increasing the likelihood of successful adoption and utilization of the secure toolchain.

Additionally, provide a list of pre-approved toolchains that meet those requirements. This approach gives developers autonomy in choosing their preferred toolchain while ensuring that security standards are met. Offering a selection of approved toolchains helps developers get started quickly and promotes adoption.

Invest in Tools and User Experience: Invest heavily in the tools that make up the secure toolchain and focus on building a user-friendly experience. Incorporate user experience (UX) principles into the toolchain to enhance usability and minimize friction for developers. When the platform team provides intuitive interfaces, clear documentation, and seamless integration with existing workflows, developers are more likely to embrace and utilize the secure toolchain.

Implement an "Error Budget" for Vulnerabilities: In traditional site-reliability engineering (SRE) an error budget sets out a “budgeted” level of production downtime, which, if breached, triggers engineering teams to shift focus from new features to improving reliability. We can use a similar approach to improve

application security: establish an "error budget" that sets a threshold for acceptable vulnerabilities or security issues within production. If this threshold is breached, developers will shift their focus from creating new features to remediating existing vulnerabilities. A vulnerability error budget can form a powerful part of your DevSecOps governance, because simply having it in place will motivate developers to improve their security practices and produce more secure code.

Incorporating these tips and tricks into your approach to driving secure toolchain adoption can help overcome resistance, foster a culture of security, and empower developers to prioritize and integrate security practices into their daily work. By aligning incentives, providing feedback loops, promoting a security-first mindset, and investing in tools and resources, organizations can successfully drive the adoption of a secure toolchain, resulting in faster and more secure software development.

Speak with a Stratascale expert in Secure Toolchains to see how we can help you move forward.